

CIVIL COVER SHEET

19cv6179

The JS 44 civil cover sheet and the information contained herein are to be used to supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the United States District Court for the Eastern District of Pennsylvania in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

John Fisher

DEFENDANTS

Wawa, Inc.

(b) County of Residence of First Listed Plaintiff New York County, NY
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant Delaware County, PA
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys (Firm Name, Address, and Telephone Number)

Barrack, Rodos & Bacine, 3300 Two Commerce Square, 2001 Market Street, Philadelphia, PA 19103, Telephone: (215) 963-0600

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
☐ 2 U.S. Government Defendant
☒ 3 Federal Question (U.S. Government Not a Party)
☒ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|
| Citizen of This State | <input type="checkbox"/> 1 | <input type="checkbox"/> 1 | Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 |
| Citizen of Another State | <input checked="" type="checkbox"/> 2 | <input type="checkbox"/> 2 | Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | Foreign Nation | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	<input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 495 Securities/Commodities/Exchange <input checked="" type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
☐ 2 Removed from State Court
☐ 3 Remanded from Appellate Court
☐ 4 Reinstated or Reopened
☐ 5 Transferred from Another District (specify)
☐ 6 Multidistrict Litigation - Transfer
☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

Subject matter jurisdiction under CAFA, 28 U.S.C. § 1332(d)

Brief description of cause:

Plaintiff alleges common law and PA UTPCPL causes of action as a result of Defendant's data breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

>\$5,000,000

CHECK YES only if demanded in complaint:

JURY DEMAND:

☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

Honorable Gene E.K. Pratter

DOCKET NUMBER

2:19cv6019

DATE

December 30, 2019

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE

DEC 30 2019

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DESIGNATION FORM

(to be used by counsel or pro se plaintiff to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: 288 Lexington Ave, Apt. #6G, New York, NY 10016

Address of Defendant: 260 W. Baltimore Pike, Wawa, PA 19063

Place of Accident, Incident or Transaction: 260 W. Baltimore Pike, Wawa, PA 19063

RELATED CASE, IF ANY:

Case Number: 2:19cv6019 Judge: Honorable Gene E.K. Pratter Date Terminated:

Civil cases are deemed related when Yes is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court?

Yes ☒ No ☐or grow out of the same transaction as a prior suit
ated action in this court?Yes ☒ No ☐ment of a patent already in suit or any earlier
eviously terminated action of this court?Yes ☐ No ☒

pus, social security appeal, or pro se civil rights

Yes ☐ No ☒☒ is / ☐ is not related to any case now pending or within one year previously terminated action in

Must sign here

PA 33729

Attorney-at-Law / Pro Se Plaintiff

Attorney I.D. # (if applicable)

B. Diversity Jurisdiction Cases:

d All Other Contracts

- ☐ 1. Insurance Contract and Other Contracts
- ☐ 2. Airplane Personal Injury
- ☐ 3. Assault, Defamation
- ☐ 4. Marine Personal Injury
- ☐ 5. Motor Vehicle Personal Injury
- ☐ 6. Other Personal Injury (Please specify):
- ☐ 7. Products Liability
- ☐ 8. Products Liability - Asbestos
- ☒ 9. All other Diversity Cases

(Please specify): CAFA 28 U.S.C. § 1332(d)

ARBITRATION CERTIFICATION

(The effect of this certification is to remove the case from eligibility for arbitration.)

Jeffrey W. Golan, counsel of record or pro se plaintiff, do hereby certify:



Pursuant to Local Civil Rule 53.2, § 3(c) (2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of \$150,000.00 exclusive of interest and costs:



Relief other than monetary damages is sought.

DEC 30 2019

DATE: 12/30/2019

Sign here if applicable

PA 33729

Attorney-at-Law / Pro Se Plaintiff

Attorney I.D. # (if applicable)

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.



**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

CASE MANAGEMENT TRACK DESIGNATION FORM

John Fisher, individually and on behalf of all
others similarly situated,

v. Plaintiff,

Wawa, Inc.,

Defendant.

CIVIL ACTION

NO.

19cv6179

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

- (a) Habeas Corpus – Cases brought under 28 U.S.C. § 2241 through § 2255. ()
- (b) Social Security – Cases requesting review of a decision of the Secretary of Health and Human Services denying plaintiff Social Security Benefits. ()
- (c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53.2. ()
- (d) Asbestos – Cases involving claims for personal injury or property damage from exposure to asbestos. ()
- (e) Special Management – Cases that do not fall into tracks (a) through (d) that are commonly referred to as complex and that need special or intense management by the court. (See reverse side of this form for a detailed explanation of special management cases.) ()
- (f) Standard Management – Cases that do not fall into any one of the other tracks. (X)

December 30, 2019

Jeffrey W. Golan, Esquire

Plaintiff John Fisher

Date

Attorney-at-law

Attorney for

(215) 963-0600

(215) 963-0838

jgolan@barrack.com

Telephone

FAX Number

E-Mail Address

(Civ. 660) 10/02

DEC 30 2019

GEKP

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JOHN FISHER, individually and on behalf of
all others similarly situated,

Plaintiff,

vs.

WAWA, INC.

Defendants.

Case No.

19cv6179

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiff John Fisher ("Plaintiff"), for himself and all others similarly situated, alleges the following against Defendants Wawa, Inc. ("Wawa" or "Defendant"). Plaintiff alleges the following based on personal knowledge as to Plaintiff and Plaintiff's own acts and on information and belief as to all other matters based upon the investigation of Plaintiff's counsel and their review of publicly available information, including news articles, press releases, Wawa's website and other publicly available information regarding the Wawa, as to all other matters.

NATURE OF THE ACTION

1. This is a data breach class action brought on behalf of a class against Wawa because of the company's failure to protect its customers' highly sensitive personally identifiable information ("PII"), including: credit and debit card numbers, expiration dates, customer names, and other data on payment cards used on Wawa's in-store payment terminals and fuel dispensers at the company's 850+ stores in six states and Washington, D.C.

2. Wawa issued a press release on its website on December 19, 2019, stating that the company had experienced a "data security incident" (the "Data Breach") that affected customer

payment card information used at potentially all Wawa locations during a specific time period. *See* An Open Letter from Wawa CEO Chris Gheysens to Our Customers, *available at* <https://www.wawa.com/alerts/data-security> (Dec. 19, 2019). The release stated that on December 10, 2019, the company discovered malware on its payment processing servers. This malware affected Wawa customers “at potentially *all*¹ Wawa locations” at some point between March 4, 2019 and December 12, 2019 (the “Class Period”). *Id.* The malware was present on most Wawa store systems by April 22, 2019, but was not identified by the company’s information security team until December 10, 2019. *Id.* The malware allowed access to credit and debit card numbers, expiration dates, and cardholder names used at Wawa payment terminals and fuel dispensers. *Id.*

3. Plaintiff used a credit card and/or debit card at one of Wawa locations during the Class Period. As a result, Plaintiff’s PII has been compromised as a result of the Data Breach. Plaintiff and other members of the Class have been placed at immediate and continuing risk of identify-theft and other related harm.

4. As a result of Wawa’s failure to safeguard its costumers highly sensitive PII, Plaintiff and other members of the class will be required to undertake expensive and time-consuming efforts to mitigate actual and potential damage from the Data Breach by, among other things, placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity. Plaintiff and other class members will also be required to purchase credit and identity monitoring services to alert them to potential misappropriation of their identity and to combat risk of further identity theft. At a

¹ Emphasis added unless otherwise noted.

minimum, Plaintiff and members of the class have suffered compensable damages because they will be forced to incur the costs associated with preventing and mitigating future loss resulting from the Data Breach.

THE PARTIES

5. Plaintiff John Fisher is a resident of New York, New York. Plaintiff made purchases using Wawa's in-store payment terminals and/or fuel dispensers at numerous Wawa locations in Pennsylvania and New Jersey between March 2019 and December 2019 with his debit and/or credit card. As such, Plaintiff's PII was stored on Wawa's payment processing servers and he was affected by the undisclosed malware. Plaintiff became aware of the Data Breach on or about December 19, 2019. On information and belief, Plaintiff's PII has been exposed and has placed him at immediate and continuing risk of identity theft-related harm.

6. Defendant Wawa is a privately held domestic New Jersey corporation with its principal executive offices located at 260 West Baltimore Pike, Wawa, Pennsylvania 19063. Wawa owns and operates more than 850 convenience retail stores (with over 600 of those stores offering gasoline) in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida and Washington, D.C. The company's stores offer "built-to-order foods, beverages, coffee, fuel services, and surcharge-free ATMS." *See* www.wawa.com. Most of its stores are open 24 hours per day, 365 days per year. *Id.* Wawa serves 800 million customers annually and has approximately \$10 billion in annual sales. *See* How Wawa Makes Money: \$10 billion in sales and other fun facts, available at <https://billypenn.com/2018/05/27/how-wawa-makes-money-10-billion-in-sales-and-other-fun-facts>.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds

\$5,000,000, exclusive of interest and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendant. The Court also has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

8. This Court has personal jurisdiction over Defendant as the company maintains its principal place of business in Wawa, Pennsylvania, is registered to conduct business in this Commonwealth, regularly conducts business in Pennsylvania, and has sufficient minimum contacts in Pennsylvania. Defendant intentionally avails itself of this jurisdiction by conducting its corporate operations here and promoting, selling, and marketing Wawa's services to resident Pennsylvania consumers and entities.

9. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

10. On December 19, 2019, Wawa announced a companywide Data Breach "at potentially *all*" of its 850+ convenience retail stores and gas stations in seven states. The company discovered malware on its payment processing servers on December 10, 2019. The malware affected customer payment card information beginning at different points in time from March 4, 2019 until it was contained on December 12, 2019.

11. Beginning at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations. By April 22, 2019, the malware was present on most store systems. The malware installed on its payment processing systems affected customers' credit and debit card numbers, expiration dates and cardholder names on cards used at in-store cash registers and/or gas pumps. According to

ZDNet, the Data Breach is one of the largest data breaches this year. *See* Wawa says POS malware incident impacts ‘potentially all locations’, available at:

<https://www.zdnet.com/article/wawa-says-pos-malware-incident-impacts-potentially-all-locations>.

B. The Data Breach Caused Harm to Plaintiff and Other Members of the Class

12. PII such as affected credit and debit card numbers, expiration dates, and cardholder names is extremely valuable data and is frequently targeted by hackers.

13. Despite well-publicized litigation and frequent public disclosures of data breaches, especially in the retail sector like the massive data breaches at Target and Neiman Marcus, Wawa did not have sufficient and adequate systems to safeguard the highly sensitive PII of Plaintiff and the other members of the class.

14. Data from payment cards is highly valuable to hackers. Hackers use stolen PII such as names and credit card numbers for a variety of financial fraud related crimes. Credit and debit card information that is stolen from the point of sale (“POS”) is known as “dumps.” Credit and debit card dumps can then be sold in the cybercrime underground. The stolen PII can be used to fraudulently clone a debit or credit card.

15. Wawa failed to implement and maintain reasonable security procedures and processes to protect the highly sensitive personal information of Plaintiff and other members of the class.

16. Both federal and state governments have established security standards and issued recommendations to prevent incidents such as the Data Breach and the resulting harm to consumers and financial institutions. For example, the Federal Trade Commission (the “FTC”), has issued numerous guides for businesses, which highlight the importance of reasonable data security practices, including PROTECTING PERSONAL INFORMATION: A GUIDE FOR

BUSINESS. *See* FEDERAL TRADE COMMISSION, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (Oct. 2016), available at <https://www.ftc.gov/tips-advice/business-center/guidance/protectingpersonal-information-guide-business>.

17. The FTC guidelines, among other things, state that business should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security issues. The FTC guidelines further recommend that businesses use an intrusion detection system to expose a breach as soon as it happens; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

18. The FTC guidelines also recommend that companies do not maintain cardholder information longer than is necessary for the authorization of a transaction; limit access to sensitive data; require the use of complex passwords on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have reasonable security measures.

19. The FTC has brought enforcement actions against companies that fail to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice in violation of Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 (2006).

20. Many states also have guidelines and/or laws governing data protection. For example, the Maryland Personal Information Protection Act, Md. Code Com Law §§ 14-3501-

3503, requires businesses such as Wawa to implement and maintain reasonable security procedures and practices to protect personal information. There are dozens of Wawas located in Maryland. Moreover, Florida law requires companies take reasonable measures to protect and secure data in electronic form containing personal information. *See* Fla. Stat. § 501.171(2). Wawa has been rapidly expanding in Florida. *See* Florida Likely to Replace New Jersey as Wawa's Largest Market, available at: [csnews.com/florida-likely-replace-new-jersey-wawas-largest-market](https://www.csnews.com/florida-likely-replace-new-jersey-wawas-largest-market).

21. Wawa did not employ reasonable and appropriate measures to protect against unauthorized access of confidential customer data. Such failure is an unfair act or practice prohibited by Section of the FTC Act, 15 U.S.C. § 45 and by the laws of various states such as Florida and Maryland. Wawa was at all relevant times fully aware of its obligation to protect the personal and financial data of its customers because of its participation in the storage of highly sensitive PII, storage of payment card data, and interactions with payment card processing networks. Moreover, Defendant Wawa was aware of the significant harm that could result if it failed to do so because Wawa collected payment card data from tens of thousands of customers daily and they knew that this data, if compromised by hackers, would result in injury to its customers, including Plaintiff and the class.

22. Despite knowing these risks, Wawa failed to take appropriate measures to safeguard its customers' PII and to take the steps necessary to protect its data network.

23. Reimbursing a consumer for financial loss resulting from a data breach is inadequate and cannot make a victim whole. A consumer who has had PII stolen and compromised may not see the full extent of harm until years after the initial data breach. Indeed, it may take years for the victim to even become aware of the theft. And, in the case of nominal

charges, typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated over and over again.

24. On information and belief, Plaintiff and other Wawa customers did not receive notification (such as an email or other communication) from Wawa other than the press release issued by the company. The malware remained on Wawa's systems for over nine months without Defendant's knowledge. Without detailed disclosures to its customers, Plaintiff and other members of the class were unknowingly and unwittingly left exposed to continued misuse and ongoing risk of misuse of their personal data for months. Plaintiff and other class members were unable to take necessary steps to safeguard their data and prevent ongoing harm.

25. Because of the Data Breach, Plaintiff and class members face years of constant monitoring and surveillance of their financial and personal information. The Data Breach also subjects Plaintiff and class members to a higher risk of phishing where hackers exploit information already obtained to access even more PII. Plaintiff and other members of the class are incurring, and will continue to incur, such damages in addition to any fraudulent credit and debit charges incurred by them and the resulting loss of their credit and access to funds, whether or not such charges are ultimately reimbursed by the bank or credit card companies.

26. The exposure of the PII of Plaintiff and other members of the class to malware was a direct and proximate result of Defendant's failure to properly safeguard and protect such information from unauthorized access, use and disclosure. Wawa failed to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and class members' PII in order to protect it against reasonably foreseeable threats to the security of such information.

27. Wawa is one of the mid-Atlantic's largest convenience and gas station chains. Therefore, it had or should have had sophisticated financial and technical resources to protect

against the Data Breach. Wawa neglected to adequately invest in data security, despite the growing number of data intrusions, especially in the retail industry, and the guidelines published by regulators.

28. Had Wawa fixed the deficiencies in its information storage and security systems; followed industry guidelines and best practices, adopted measures recommended by the FTC and experts in the field, and adhered to state law (such as Florida and Maryland), Wawa would have prevented the Data Breach and the malware on its payment storage and security system and, ultimately, the theft of Plaintiff's and class members' confidential PII.

29. As a direct and proximate result of Wawa's wrongful actions and inaction, Plaintiff and class members have suffered immediate and continuing risk of harm from identity theft and fraud, requiring them to take the time and effort to mitigate both actual and potential harm from the Wawa Data Breach, by, among other things, placing "freezes" and "alerts" with credit reporting and monitoring agencies, contacting their financial institutions, closing and/or modifying credit card and bank accounts, and closely reviewing and monitoring their credit reports and accounts for suspicious or unauthorized activity.

30. Wawa's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. The improper disclosure, compromising and theft of their PII;
- b. Unauthorized charges on credit and/or debit card accounts;
- c. The imminent and impending injury flowing from potential fraud and identity theft posed by PII being accessed by hackers and unauthorized parties and misused by the sale of PII on the Internet black market and dark web;

- d. The untimely and inadequate notification of the Data Breach;
- e. Loss of privacy;
- f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;
- g. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;
- h. Loss of use of, and access, to funds in their accounts and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were allowed to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and
- i. The loss of productivity and value of their time spent to address, attempt to ameliorate and/or mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

31. Despite the fact that Plaintiff's and other class members' data has been stolen, Wawa continues to store PII on their payment servers. Since Wawa has demonstrated an inability to prevent a data breach or stop it from continuing, Plaintiff and class members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to ongoing and further theft.

32. Wawa has "arranged with Experian to provide potentially impacted customers with one year of identity theft protection and credit monitoring at no charge" as a result of the

Data Breach. See <https://www.wawa.com/alerts/data-security>. But, as previously detailed above, the PII of Plaintiff and other class members may exist on the dark web for years before it is purchased and used by hackers. One year of monitoring and no insurance or other protection is inadequate to protect Plaintiff and the members of the class against the real and long-term threats against their PII. Therefore, Plaintiff and class members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

CLASS ACTION ALLEGATIONS

33. Plaintiff, John Fisher, brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and all others similarly situated, as representative of the following Class:

All persons residing in the United States who provided PII to Defendant and whose PII was accessed, compromised, or stolen as a result of the Data Breach disclosed by Defendant on December 19, 2019.

34. The aforementioned class is referred to herein as the “Class”.

35. Excluded from the Class are affiliates, predecessors, successors, officers, directors, agents, servants, or employees of Defendants, and the immediate family members of such persons. Also excluded are any trial judge who may preside over this action and their law clerks, court personnel and their family members, and any juror assigned to this action.

36. Plaintiff reserves the right to amend the definition of the Class if discovery and/or further investigation reveal that it should be modified.

37. The members of the Class are so numerous that the joinder of all members of the Class in a single action is impractical. While the exact number of the Class members is unknown to Plaintiff at this time, Wawa has acknowledged that its customers' PII was compromised for over nine months. Therefore, it stands to reason that the number of Class members is likely in

the millions. The Class members are readily identifiable from information and records in the Defendant's possession, custody, or control, such as transaction records and purchases.

38. There are common questions of law and fact to the Class members, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- a. Whether Defendant owed a duty to Plaintiff and Class members to safeguard and protect the security of their PII;
- b. Whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiff and Class members' PII;
- c. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and Class members' PII from unauthorized capture, dissemination, and misuse.

39. Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every Class member, was misused and/or improperly disclosed by Defendant.

40. Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained competent counsel experienced in litigation of complex class actions, including consumer class actions. Plaintiff intends to prosecute this action vigorously.

41. Plaintiff's claims are typical of the claims of all of the other Class Members, and Plaintiff has the same non-conflicting interests as the other Class members. Therefore, the interests of the Class members will be fairly and adequately represented by Plaintiff and his counsel.

42. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted

claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting damages in the aggregate would go un-remedied.

43. Class certification is appropriate here under Fed. R. Civ. P. 23(a) and (b)(2a) because Defendant has acted or refused to act on grounds generally applicable to the Class, such that final injunctive or corresponding declaratory relief is appropriate to the Class as a whole.

CLAIMS FOR RELIEF

COUNT 1

(Negligence)

44. Plaintiff repeats, re-alleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

45. Wawa owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties.

46. This duty included, among other things, designing, maintaining, and testing Wawa's security systems to ensure that Plaintiff's and Class members' PII was adequately secured and protected. Wawa further had a duty to implement processes that would detect a breach of the company's security system in a timely manner.

47. Wawa also had a duty to timely disclose to Plaintiff and Class members that their PII had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiff and Class members could take appropriate measures to cancel or change their credit or debit cards, to begin monitoring their accounts for

suspicious activity or unauthorized access, to contact the credit bureaus to request freezes or place alerts, and take all other necessary and appropriate measures and precautions.

48. Wawa breached its duty to exercise reasonable care in safeguarding and protecting Plaintiffs and Class Members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information; allowing unauthorized access to Plaintiff's and Class members' PII stored by Wawa, and failing to recognize in a timely manner the breach.

49. Wawa breached its duty to timely disclose that Plaintiff's and Class members' PII had been, or was reasonably believed to have been, stolen or compromised.

50. Wawa's failure to comply with industry regulations and the delay between the date of intrusion and the date Wawa informed customers of the Data Breach further evidence Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII.

51. But for Wawa's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII would not have been compromised, stolen, and viewed by unauthorized persons.

52. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII. Wawa knew or should have known that their systems and technologies for processing and securing Plaintiff's and Class members' PII had security vulnerabilities susceptible to malware and hackers.

53. As a result of Wawa's negligence, Plaintiff and Class members incurred damages including, but not limited to, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Wawa's security failures; the

value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit and debit cards of Wawa's customers by identity thieves who wrongfully gained access to the PII of Plaintiff and Class members.

COUNT II
(Negligence Per Se)

54. Plaintiff repeats, re-alleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

55. Section 5 the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Wawa's failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Wawa's duty.

56. Wawa violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class members' PII and not complying with industry standards. Wawa's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach at one of the mid-Atlantic's largest convenience store and gas station chains.

57. Wawa's violation of Section 5 of the FTC Act constitutes negligence *per se*.

58. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

59. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty

enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

60. As a direct and proximate result of Wawa's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
(Breach of Implied Contract)

61. Plaintiff repeats, re-alleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

62. When Plaintiff and Class members paid money and provided their PII to Wawa in exchange for goods and services, they entered into implied contracts with Wawa pursuant to which Wawa agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

63. Wawa solicited and invited prospective consumers such as Plaintiff and Class members to provide their PII as part of its regular business practices by using their credit and/or debit cards. Plaintiff and Class members accepted Wawa's offers and provided their PII to Wawa.

64. In entering into such implied contracts, Plaintiff and Class members assumed that Wawa's data security practices and policies were reasonable and consistent with industry standards, and that Wawa would use part of the funds received from Plaintiff and Class members to pay for adequate and reasonable data security practices.

65. Plaintiff and Class Members would not have entrusted their PII to Wawa in the absence of the implied contract between them and Wawa to keep the information secure.

66. Plaintiff and Class members fully performed their obligations under the implied contracts with Wawa.

67. Wawa breached their implied contracts with Plaintiff and Class members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their PII was compromised as a result of the Data Breach.

68. As a direct and proximate result of Wawa's breaches of their implied contracts, Plaintiff and Class members sustained actual losses and damages, including, but not limited to, out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Wawa's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit and debit cards of Wawa's customers by identity thieves who wrongfully gained access to the PII of Plaintiff and Class Members.

COUNT IV

**(For Violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Laws)
72 P.S. § 201-1 *et seq***

69. Plaintiff repeats, re-alleges, and incorporates by reference the allegations contained in each and every paragraph above, as though fully stated herein.

70. As a consumer of Wawa's services, Plaintiff is authorized to bring a private action under Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTCPL"). 73 P.S. § 201-9.2.

71. Plaintiff is a "person" within the meaning of 73 P.S. § 201-2(2).

72. Plaintiff and Class Members provided their PII to Wawa pursuant to transactions in “trade” and “commerce” as meant by 73 P.S. §201-2(3), for personal, family, and/or household purposes.

73. The UTPCPL prohibits “unfair or deceptive acts or practices in the conduct of any trade or commerce[.]” 73 P.S. § 201-3.

74. This Count is brought for Wawa’s unfair and deceptive conduct, including Wawa’s unlawful and unfair and deceptive acts and practices, which “creat[ed] a likelihood of confusion or of misunderstanding” for Plaintiff and Class members as meant by 73 P.S. § 201-2(4)(xxi).

75. Wawa engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale and advertisement of the goods purchased by Plaintiff and the Class in violation of 73 P.S. § 201-3, including but not limited to the following:

a. Wawa failed to enact adequate privacy and security measures to protect Plaintiff’s and Class members’ PII from unauthorized disclosure, release, data breaches, malware and theft, which was a direct and proximate cause of the Data Breach;

b. Wawa negligently represented that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff’s and Class members’ PII from unauthorized deceptive disclosure, release, data breaches, malware and theft was unfair and deceptive given the inadequacy of its privacy and security protections; and

c. Wawa’s negligence in failing to disclose the material fact of the inadequacy of its privacy and security protections for Plaintiff and Class Members was unfair and deceptive.

76. The above unfair and deceptive acts and practices by Wawa were immoral, unethical, and unscrupulous. These acts caused substantial injury to consumers that the

consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

77. Wawa knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiffs Class members' PII and that risk of a data breach or theft was highly likely. Wawa's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and reckless with respect to the rights of members of the Class.

78. Plaintiff and Class Members relied on Wawa's unfair and deceptive acts and practices when they paid money in exchange for goods and services and provided their PII through Wawa's in-store payment terminals and fuel dispensers.

79. Plaintiff and Class members relied on Wawa to safeguard and protect their PII and to timely and accurately notify them if their data had been breached and compromised.

80. Plaintiff and Class members seek all available relief under the UTPCPL, 73 P.S. § 201-1 *et seq.*

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, John Fisher, individually and on behalf of the Class, respectfully requests that the Court:

A. Certify the Class pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class members;

B. Designate Plaintiff as representative of the Class and the undersigned counsel, Barrack, Rodos & Bacine, as Class Counsel;

C. Award Plaintiff and the Class compensatory damages in an amount to be determined by the Court and treble and punitive damages to punish Defendant's egregious conduct as described herein, and to deter Defendant and others from engaging in similar conduct;

D. Award Plaintiff and the Class injunctive relief, as permitted by law or equity, including enjoining Defendant from continuing the unlawful practices set forth herein, ordering Defendant to fully disclose the extent and nature of the security breach and theft, and ordering Defendant to pay for not less than three years of identity theft and credit card monitoring services for Plaintiff and the Class;

E. Award Plaintiff and the Class statutory interest and penalties;

F. Award Plaintiff and the Class their costs, prejudgment and post judgment interest, and attorneys' fees; and

G. Grant such other relief that the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury as to all issues stated herein, and all issues so triable.

Dated: December 30, 2019

BARRACK, RODOS & BACINE

By: 

Julie B. Palley
Chad A. Carder
Jeffrey B. Gittleman
Jeffrey W. Golan (PA #33729)
3300 Two Commerce Square
2001 Market Street
Philadelphia, PA 19103

and

Stephen R. Basser
One America Plaza
600 W. Broadway, Suite 900
San Diego, CA 92101

Attorneys for Plaintiff John Fisher